National Association of Federal Credit Unions
3138 10th Street North • Arlington, VA 22201-2149
(703) 522-4770 • (800) 336-4644 • Fax (703) 524-1082
www.nafcu.org • nafcu@nafcu.org

January 19, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Identity Theft Task Force

Dear Sir or Madam:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association that exclusively represents the interests of our nation's federal credit unions (FCUs), I am responding to the Federal Identity Theft Task Force's (Task Force) request for public comment on ways to improve the effectiveness and efficiency of federal government efforts to reduce identity theft.

The Task Force, chaired by Attorney General Alberto Gonzales, and co-chaired by Federal Trade Commission Chairman Deborah Platt Majoras, was established by an Executive Order on May 10, 2006, and was specifically directed to develop a coordinated strategic plan to combat identity theft, and to recommend ways to improve the effectiveness and efficiency of federal efforts to improve identity theft awareness, prevention, detection, and prosecution. As it prepares a final strategic plan for the President, the Task Force is seeking comment on ways to make criminal prosecution of identity theft more effective; how to better protect sensitive consumer information in the public and private sectors and improve guidance for consumers and the business community; and ways to assist consumers following breaches or misuse of their personal information.

Identity theft continues to be a major threat to and a significant concern for American consumers. Identity theft costs time and money for financial institutions and may create significant risks to safety and soundness. Even worse, such fraud wreaks havoc on its victims by destroying credit histories, violating financial privacy, and ruining good names. The credit union industry is firmly committed to combating identity theft. NAFCU and its member credit unions believe that credit unions must continue to be vigilant and proactive in helping to protect their

members from this serious financial crime; as such, we would like to take the opportunity to submit the following comments.

Maintaining Security of Consumer Data

Data Security

The Task Force is considering whether to recommend that national data security requirements be imposed on all businesses and commercial entities that maintain sensitive consumer information.

NAFCU member credit unions have raised concerns about the increasing level of responsibility being placed on financial institutions to prevent and mitigate identity theft and to bear the significant costs for fraud losses. NAFCU believes that the war against identity theft must be fought on several fronts and that there must be a coordinated effort to combat this crime. Accordingly, NAFCU strongly urges the Task Force to recommend increased liability for merchants, businesses, and other unregulated organizations that compromise consumer data security.

The credit union community is already extremely vigilant in guarding its members against identity theft. Credit unions, as well as other financial depository institutions, are required to comply with a litany of laws and regulations designed for the protection, detection, prevention, and mitigation of identity theft. These laws and regulations serve not only to protect consumers, but also help financial institutions to mitigate fraud losses, since it is ultimately the institution that bears the cost of losses due to the crime. For example, pursuant to the Gramm-Leach-Bliley Act (GLBA), credit unions are required to implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. *See* 12 CFR part 748, Appendix A. Credit unions are also required to notify members of any incidence of unauthorized access or use of confidential member information if harm to the member has happened or is likely to occur. *See* id., Appendix B.

Recently, credit unions and other federal depository institutions have also implemented Federal Financial Institutions Examination Council (FFIEC) guidance requiring appropriate authentication tools, including multi-factor systems or layered security, to verify the identity of new members and authenticate the identity of existing members that access electronic or web-based financial services. *See* NCUA Letter to Credit Unions 05-CU-18.

In addition, financial institutions will likely soon be required by regulation to establish a risk-based written Identity Theft Prevention Program containing reasonable policies and procedures to address the risk of identity theft. The jointly proposed regulation, which would implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act), Pub. L. 108-159 (2003), also includes guidelines for financial institutions and creditors to identify "red flags" which might indicate a possible identity theft. *See* 71 Fed. Reg. 40786 (July 18, 2006).

Thus, the continued prevalence of identity theft must not be attributed to the deficiencies of financial institutions. Rather, the problem lies with the unregulated businesses that fail to implement the necessary data security controls to adequately protect American consumers. Indeed, data from NAFCU's January 2007 *Flash Report* survey indicates that 27 percent of responding credit unions suffered some form of a data security breach in 2005 or 2006, but more notably, that most of these breaches occurred via merchants and processors. Among these credit unions, 86 percent had to reissue credit, debit, and/or ATM cards in 2005 and 2006 due to these breaches. In 2006, the average cost to credit unions for replacing each member's credit card was $6.60, and the average cost for replacing each member's debit card was $5.79. Overall, for last year alone, the average cost per breach per credit union was $4,600.

Accordingly, NAFCU believes that uniform and comprehensive national data security requirements, similar to those already imposed on financial institutions pursuant to the GLBA and other laws, should be applied to all business entities that maintain private consumer information. Greater parity is crucial to ensuring that merchants and businesses are battling identity theft with the utmost vigilance, and that fraudsters are prevented from exploiting sensitive consumer data.

Education of Consumers on Safeguarding Data

The Task Force is also considering whether it is necessary to better educate the private sector and consumers on safeguarding sensitive information and about the types of responses that would be appropriate in the event of a data breach.

NAFCU member credit unions have long recognized the importance of financial literacy and education. Credit unions are among the forerunners of financial education in America and are proud to be proactively involved in promoting financial literacy across the nation. Indeed, education and volunteerism embodies the guiding principle of the credit union system—"People Helping People." For example, many credit unions provide free educational seminars or individual financial counseling, and provide their membership with helpful information about identity theft via newsletters and statement inserts.

Recognizing the national need for identity theft training, NAFCU provides model curriculums and access materials to help meet recommended education requirements set out by the FFIEC. For instance, statement inserts provided to our members (e.g., *Don't Get Phished*; *Internet Safety* Tips; and *Tools to Prevent Identity Theft*) help meet FFIEC education recommendations regarding Internet authentication guidance. NAFCU has also held several identity theft seminars for credit union staff and credit union members, to include one featuring Wayne Abernathy, then Treasury Assistant Secretary for Financial Institutions, and participated in the Treasury Department video: *Identity Theft: Outsmarting the Crooks*.

Given today's complex realities, it is crucial that consumers are not only literate about financial management, but also knowledgeable about ways to safeguard their personal financial data. NAFCU strongly supports federal efforts to provide comprehensive financial education for all Americans, and asks the Task Force to support activities that would increase awareness of the importance of data security within the business community and among individual consumers. In

particular, NAFCU supports the creation of a national public awareness campaign to educate private organizations about how to prevent and detect identity theft, and to arm consumers with the tools necessary to protect themselves from fraud. NAFCU urges the Task Force to incorporate existing credit union and trade association education efforts into a national strategy.

Law Enforcement: Prosecuting and Punishing Identity Thieves

NAFCU also encourages the Task Force to support any congressional efforts to strengthen criminal penalties against identity thieves. Financial institutions should not bear the burden of policing this criminal activity. While the credit union community remains committed to continuing to assist law enforcement by providing important identity-theft related records and information, NAFCU firmly believes that aggressive prosecution and tough punishment of identity thieves is crucial to eradicating this devastating crime.

NAFCU appreciates this opportunity to share its comments on this important issue and would like to commend the Task Force on its efforts in combating this serious crime. Should you have any questions or require additional information please call me or Pamela Yu, NAFCU's Associate Director of Regulatory Affairs, at (703) 522-4770 or (800) 336-4644 ext. 218.

Sincerely,

Fred R. Becker, Jr.
President/CEO

FRB/py/crh